PAT-NO: JP358114134A
DOCUMENT-IDENTIFIER: JP 58114134 A
TITLE: RANDOM NUMBER GENERATOR

PUBN-DATE: July 7, 1983

INVENTOR-INFORMATION:

NAME	COUNTRY
KOSUGI, HISANOBU	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
HITACHI ELECTRONICS ENG CO LTD	N/A

APPL-NO: JP56209631
APPL-DATE: December 28, 1981

INT-CL (IPC): G06F007/58

US-CL-CURRENT: 708/250

ABSTRACT:

PURPOSE: To set automatically an initial **value to generate easily high-quality random numbers, by providing a random number generation processing program in a calculator and setting the counted vlaue of a counter as the initial value of the random number generation processing when an initial value setting request is issued at the program operation time**.

CONSTITUTION: The clock output from a clock oscillator 1 is applied to a counter 2 as a program counter and a counter 3 as a watchdog timer and is counted successively in accordance with respective purposes. Clocks from the oscillator 1 are applied to a counter 4 for the random number processing, and the counted value is taken into this counter 4 by the designation of a random number processing routine F. This routine F is a kind of processing routine in the calculator and is accessed when the random number processing is requested. The **counter 4 is used as an interval timer, and the counted value of the counter 4 is set as the initial value when the initial value setting is requested at the program operation time, and**

the random number generation processing is processed by the successive calculation method due to the mixed congruence method.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-312078
(43)Date of publication of application : 09.11.1999

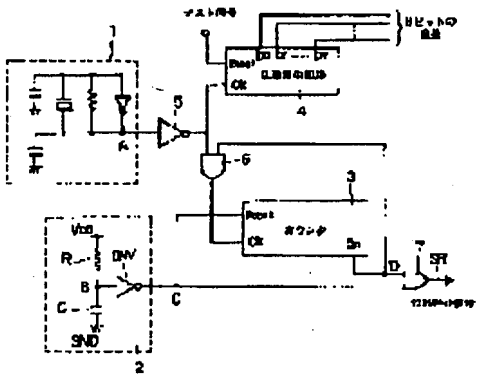
(51)Int.Cl. G06F 7/58
G06F 1/04

(21)Application number : 10-120757
(22)Date of filing : 30.04.1998

(71)Applicant : ROHM CO LTD
(72)Inventor : TAGIRI HIROKAZU

(54) SEMICONDUCTOR DEVICE HAVING RANDOM NUMBER GENERATING CIRCUIT

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent random numbers from being equal at all the time by starting operation of a random number generating circuit without applying an initial value after a power source is turned on wherein the number of clocks to be inputted for a fixed time from the start of operation is not determined.
SOLUTION: After power source is turned on and an oscillation circuit 1 is stabilized, resetting of an entire system is released, and after the lapse of a prescribed time, random numbers are read out. Thus, after resetting of the entire system is released, random numbers are always read out at the same timing. But, a random number generating circuit 4 is not initialized after the power source is turned on and further, the oscillation circuit 1 is started while its oscillation waves are unstable, so the operation is started without an initial value, and the number of clocks inputted for the lapse of a fixed time from the start of operation is not determined and random numbers are different at all the time.



LEGAL STATUS

[Date of request for examination] 14.10.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the semiconductor device which has the random-number-generation circuit which outputs the random number of a predetermined sequence synchronizing with an input clock.
[0002]
[Description of the Prior Art] Usually, in the system, in order to secure operational stability to it, while initializing the whole system to it, the case of the system which has the random-number-generation circuit to which reset is applied (it is not made to operate), and which is like and outputs a random number was the same as that of it until the oscillation of a clock was stabilized in the power up.
[0003]
[Problem(s) to be Solved by the Invention] When the random-number-generation circuit which outputs a random number is a counter configuration (configuration which outputs the random number of a predetermined sequence synchronizing with an input clock) here, the value of the random number obtained to the same timing after reset discharge is surely the same.
[0004] Moreover, after reset discharge, by the number of counts of an input clock, a random number will be read and a random number will usually be read to the always same timing in the circuit which uses a random number.
[0005] As mentioned above, in the conventional random-number-generation system which has a random-number-generation circuit, when a random-number-generation circuit is a counter configuration, the random number read immediately after powering on by the circuit which uses a random number will become the always same value.
[0006] Then, this invention is a semiconductor device which has the random-number-generation circuit of a counter configuration, and aims at offering the semiconductor device with which it was made for the value of the random number read by the circuit which uses a random number immediately after powering on not to become always the same.
[0007]
[Means for Solving the Problem] The oscillator circuit which generates the clock signal for carrying out synchronous operation of the semiconductor integrated circuit in this invention in order to attain the above-mentioned purpose, The initialization circuit which generates the reset signal for making the logic state of said semiconductor integrated circuit decide, It is the semiconductor device which has the random-number-generation circuit which generates the random number of a predetermined sequence synchronizing with said clock signal. Said random-number-generation circuit While not being initialized by said reset signal, said clock signal is made to be inputted also in the condition with unstable actuation of said oscillator circuit.
[0008] The number of the clocks inputted after a random-number-generation circuit starts actuation after powering on, without being given the initial value of the random number to output and starting actuation by the above configuration before fixed time amount passes becomes unfixed, and even if it is the same

timing after reset discharge of the whole (except for a random-number-generation circuit) system, the random number outputted from a random-number-generation circuit does not serve as the always same value.

[0009]

[Embodiment of the Invention] Below, the operation gestalt of this invention is explained, referring to a drawing. Drawing 1 is drawing showing the configuration of the semiconductor device which is 1 operation gestalt of this invention. this drawing -- setting -- 1 -- for a counter and 4, as for an inverter circuit and 6, the random-number-generation circuit of a counter configuration and 5 are [the oscillator circuit of crystal, and 2 / a power-on-reset circuit and 3 / an AND circuit and 7] OR circuits.

[0010] The oscillation wave of an oscillator circuit 1 is inputted into the clock terminal CK and AND circuit 6 of the random-number-generation circuit 4 through an inverter circuit 5. Output terminal of the counter 3 constituted by another input of AND circuit 6 as a binary counter of N bit - Qn is connected and the output of AND circuit 6 is connected to the clock terminal CK of a counter 3.

[0011] The output of the power-on-reset circuit 2 is connected to the input of OR circuit 7 while connecting with the reset terminal Reset of a counter 3. In another input of OR circuit 7, it is the output terminal of a counter 3. - Qn is connected.

[0012] And the output (it is hereafter called "the system-reset signal SR") of OR circuit 7 The circuit which is inputted into the circuit (un-illustrating) which uses the random number which the random-number-generation circuit 4 outputs, and uses this random number If the predetermined number count of the clock inputted is carried out after system-wide reset is canceled (after the system-reset signal SR is set to a low level from high level) The random number which the random-number-generation circuit 4 outputs will be read, and a random number will be read to the always same timing.

[0013] Although the node of Resistance R and Capacitor C by which the series connection was carried out to supply voltage VDD between Glands GND is connected to the input of Inverter INV and the output (output side of Inverter INV) becomes high-level immediately after powering on, the power-on-reset circuit 2 will switch to a low level, if the predetermined time t0 decided by Capacitor C and Resistance R passes.

[0014] A counter 3 is an output terminal in a reset condition (condition that the signal inputted into the reset terminal Reset is high-level). - It is an output terminal when the count count of predetermined of the standup of the clock inputted into the clock terminal CK after reset discharge (after the signal inputted into the reset terminal Reset switches from high level to a low level) is carried out, although the output from Qn is made high-level. - The output from Qn is switched to a low level.

[0015] In addition, the count which counts the standup of the clock which a counter 3 inputs from the clock terminal CK is the output terminal of a counter 3. - After powering on, after the oscillation wave of an oscillator circuit 1 is stabilized by the output from Qn, it is set up so that it may switch to a low level.

[0016] The random-number-generation circuit 4 is a counter configuration as shown in drawing 3 . In this example Cascade connection of the eight flip-flops FF1-FF8 is carried out. The inside between such cascade connection, Between a flip-flop FF 2 and a flip-flop FF 3, between a flip-flop FF 3 and a flip-flop FF 4, and between a flip-flop FF 5 and a flip-flop FF 6 The EXOR circuits G1 and G2 and G3 were prepared, respectively, and the output of the last stage has returned to the input of the flip-flop FF 1 of the first rank, and each EXOR circuit G1 - G3. By this, in 8 bits which consists of inputs of each stage, the random number of a predetermined sequence will appear synchronizing with the clock inputted into the clock terminal CK.

[0017] In addition, although the initial value which the random-number-generation circuit 4 has the reset terminal Reset, and reset starts with the signal inputted into this reset terminal Reset, and is outputted as a random number is given Inside a system, it does not connect anywhere, but for the purpose of judging whether it is operating normally etc., this reset terminal can input a signal into a reset terminal from the exterior, and can apply reset now to the random-number-generation circuit 4 from the exterior only at the time of a test.

[0018] As mentioned above, the oscillation wave A of an oscillator circuit 1 behind powering on, the

electrical potential difference of the capacitor C of the power-on-reset circuit 2, and the node B with Resistance R, If the output C of the power-on-reset circuit 2, the output D of a counter 3, and the timing chart of the system-reset signal SR come to be shown in drawing 2 and time amount t0+t1 passes after powering on That is, after the oscillation of an oscillator circuit 1 is stabilized, system-wide reset is canceled, and when time amount t2 passes further, a random number will be read after that. In addition, the time amount which takes the time amount it is decided by the capacitor C of the power-on-reset circuit 1 and Resistance R that t0 will be, and t1 for a counter 3 to carry out the count count of predetermined of the standup of a clock, and t2 are time amount taken for the circuit which uses a random number to carry out the predetermined number count of the clock.

[0019] Therefore, although a random number will be read to the always same timing after system-wide reset is canceled With this operation gestalt, about the random-number-generation circuit 4 After powering on, without initializing in the condition with the still more unstable oscillation wave of an oscillator circuit 1 The number of the clocks inputted after starting actuation and starting actuation, without being given initial value before fixed time amount passes, since actuation is made started becomes unfixed, and, thereby, the value of the random number read immediately after powering on does not become always the same.

[0020] In addition, although the value of the random number outputted to a power up may become the same according to the imbalance of the capacity of a transistor etc. about the random-number-generation circuit of a counter configuration even if it does not apply reset Even in such a case, with this operation gestalt, since he is trying for an input clock to make it operate from an unstable condition further The number of the clocks which will be inputted by the time fixed time amount passes is unfixed after powering on, and the value of the random number read by the circuit which uses a random number does not become always the same.

[0021] Furthermore, with this operation gestalt, since time amount until the output of the power-on-reset circuit 2 changes with dispersion in Capacitor C and Resistance R from high level to a low level after powering on, as a result time amount until a system reset is canceled vary, the values of the random number read after powering on by the circuit which uses a random number differ for every system.

[0022] In addition, this invention is not limited to the above-mentioned operation gestalt, and can take various configurations about an oscillator circuit 1, the power-on-reset circuit 2, a counter 3, and the random-number-generation circuit 4. Moreover, about an oscillator circuit 1 and the power-on-reset circuit 2, even if it is the interior of IC and is IC exterior, neither is available.

[0023]

[Effect of the Invention] As explained above, according to the semiconductor device of this invention which has a random-number-generation circuit Since the number of the clocks inputted after a random-number-generation circuit starts actuation after powering on, without being given initial value and starting actuation before fixed time amount passes becomes unfixed After system-wide (except for a random-number-generation circuit) reset is canceled, even if a random number is read to the same timing, it is lost that the value becomes always the same.

[Translation done.]